BY ORDER OF THE COMMANDER
TRAVIS AIR FORCE BASE

TRAVIS AIR FORCE BASE
INSTRUCTION 10-105

1 MARCH 2003

Operations

OPERATIONS SECURITY (OPSEC) PROCEDURES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: 60AMW/XPO (TSgt Gregory Atkins)

Certified by: 60AMW/XP (Lt Col Keith A. Albrecht)

Supersedes TAFB Instruction 10-105, 1 February 1999

Pages: 8
Distribution: L

This instruction implements Air Force Policy Directive (AFPD) 10-11, *Operations Security*; and Air Force Instruction (AFI) 10-1101, *Operations Security (OPSEC) Instructions*. It establishes an OPSEC program, including specific applications of those guidelines and requirements for Travis Air Force Base (TAFB). It applies to all TAFB and tenant unit personnel assigned or attached to TAFB and the 349th Air Mobility Wing.

SUMMARY OF REVISIONS

A revision was made to TAFB Instruction 10-105 to reflect changes in the 60th AMW organizational structure and force protection terminology. **A bar (|) indicates a change since the last edition.**

1. General Information.

1.1. Critical Information (CI) is generally UNCLASSIFIED, sensitive information about friendly (U.S., Allied, and/or coalition) activities, intentions, capabilities, or limitations that an adversary needs in order to gain a military, political, diplomatic, or technical advantage. Individual CI items may not be harmful, but in aggregate a trained analyst may be able to interpret or extract enough information to cause mission degradation.

1.2. The OPSEC concept, and the program within which it is applied, aims at countering the worldwide multi-discipline and evasive adversary threat to the security of United States (US) military installations, personnel and activities. The total threat results from multiple and overlapping collection efforts targeted against all productive sources of information. Adversaries may use a broad array of sophisticated collection resources to target US participants and activities.

1.3. Information related to strategic activities and Air Mobility Command (AMC) support of these activities is abundant in unclassified literature. The news media present another category of risk con-

cerning US operations. It is entirely possible that on-the-scene reporters, complete with live television coverage, could transmit US preparations via satellite. Remember that just because the media has reported something, the information could still be sensitive, and the media could be looking for *confirmation* from the military.

1.4. Use only Public Affairs (PA) channels when dealing with the media.

2. OPSEC Vulnerabilities and Protective Measures.

2.1. OPSEC vulnerabilities are weaknesses in security measures, operational practices, and/or procedures that could be exploited. In order for a true vulnerability to exist, an adversary must have both the intent and capability to exploit the weakness. During a contingency situation, hostile intelligence services may increase collection efforts.

2.2. Protective measures prevent detection, affect observation and interpretation, and avert attention away from an operation/activity. Functional managers, unit commanders/chiefs, and unit OPSEC Program Managers should implement unit developed protective measures to reduce the signature of increased activity on Travis AFB due to contingency operations and/or OPLAN implementation.

2.2.1. Protective measures should not unnecessarily inhibit unit actions resulting in wasted effort or mission degradation.

2.2.2. Examples of effective protective measures include, but are not limited to:

2.2.2.1. Not using a cellular or cordless telephone to discuss CI items (consider using a STU-III telephone).

2.2.2.2. Shredding CI items once no longer needed, with a shredder approved for Privacy Act Information.

2.2.2.3. Not leaving a logged-on computer unattended for extended periods of time.

2.2.2.4. Not discussing contingency details in a public place (off-base, Base Exchange, food-court, etc.).

2.2.2.5. Whenever possible, use ongoing exercises as a cover for initiation of contingency operations.

2.2.2.6. Use darkness and/or adverse weather to mask force generation or deployment.

2.2.3. OPSEC plays a vital role and should be stressed during all phases of contingency operations.

3. Critical Information.

3.1. **Attachment 2** provides general guidance concerning 60 AMW Critical Information items and the AMC CI items. Individuals should review and familiarize themselves with the following listing

and their unit specific CI items. Each Unit OPSEC Program Manager should develop specific CI listings for their organization.

DENNIS M. MCCARTHY, Col, USAF
Director of Wing Staff

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Air Force Policy Directive 10-11, *Operations Security*

AFI 10-1101, *Operations Security (OPSEC) Instructions*

Attachment 2

CRITICAL ITEMS

MISSION (General)

Subject Requiring Protection (refer to paragraph 2.2.2. for protective measures)	**During Which Phase**			
	Plan	**Prep**	**Exec**	**Post**
Information indicating mission capability (not limited to LIMFACS)	**X**	**X**		
Indications that troop deployment is being considered or underway.	**X**	**X**	X	
Detailed breakout of participating TAFB forces relating to a contingency operation	**X**	**X**	X	
Aircraft configured for special weapons movements and/or logistics support for such movements	**X**	**X**	X	
Materials/information containing CODE NAMES of operations	**X**	**X**	X	

PLANNING ACTIVITIES

Subject Requiring Protection (refer to paragraph 2.2.2. for protective measures	**During Which Phase**			
	Plan	**Prep**	**Exec**	**Post**
Tasked organizations	**X**	**X**		
Sequence of events (SOE) and load planning information	**X**	**X**		
Supply, maintenance, transportation and logistics requirements	**X**	**X**		
			X	X

Existence of a particular war or contingency plan, its mission and circumstances under which the plan would be executed	**X**	**X**		
Identity, strength, and readiness of TAFB forces available for immediate employment and deployment to a contingency or combat area	**X**	**X**	X	
Capability of TAFB to support sustained combat/ contingency operations	**X**	**X**	X	X
Vulnerability to sabotage/penetration (both physical and in cyberspace)	**X**	**X**	X	X
Information relating to 60 AMW and/or HHQ deception planning	**X**	**X**	X	X
Information or indicators pertaining to impending air activities in areas of international tension, conflict or contingency	**X**	**X**	X	X
Tasking of tanker/airlift and the deployment locations under contingency and/or war plans	**X**	**X**	X	
Future programming activities that would improve aircraft and command and control capability	**X**	**X**	X	X
Increased alert status of TAFB and/or AMC forces	**X**	**X**	X	

COMMUNICATIONS

Subject Requiring Protection (refer to paragraph **2.2.2.** for protective measures)	**During Which Phase**			
	Plan	**Prep**	**Exec**	**Post**
Communications support that is unique to a particular type of war or contingency operation	**X**	**X**	**X**	**X**

Compromises of any encryption/encoding systems or COMSEC violations	X	X	X	X
Major difficulties or extended outages involving TAFB command, control and communications	X	X	X	X

SUPPORT ACTIVITIES

Subject Requiring Protection (refer to paragraph 2.2.2. for protective measures)	**During Which Phase**			
	Plan	**Prep**	**Exec**	**Post**
Rights and privileges at staging areas, airfields, and logistic points	X	X	X	
Contingency area weather information	X	X	X	
Information concerning a buildup of supplies, equipment, or personnel in support of a specific operation	X	X	X	
Aircraft operational readiness status rates	X	X	X	X
Departure reliability of operational aircraft	X	X		
Activation of Unit Control Cells (UCCs) or Group Control Cells (GCCs)	X	X	X	
Activation of Crisis Action Team (CAT)	X	X	X	
Relocation of CAT and/or Command and Control activities (CP or Control Centers)	X	X	X	
Indication of movement of official VIP/DV passengers, aircraft or vehicles	X	X		

AMC Critical Information List

AMC has identified the key items of friendly activities or intentions that need special consideration in selecting means of communication and protection:

Specific mission nature and objectives.
CJCS Alert/Warning Orders, date/time of execution, deployment/routes, staging, and operating locations.
Implementing conditions (i.e., DEFCON, FPCON, INFOCON, WEATHER).
Capabilities and limitations.
Identity, strength, disposition, readiness, and command relationships of forces involved (includes personnel/equipment/supplies).
Potential circumstances that generate a particular operation, including planning/execution/ reaction times.
Planning and programming activities that would enhance AMC Mission Effectiveness.
Critical communications and computer systems locations, support, techniques, limitations, effectiveness, and outages that support AMC missions.
Movement of key personnel (includes VIPs and DVs).
Effect of Adversary activities and operations.
Deception capability, use, and techniques.

NOTE: While protection of the CI items listed above is paramount, it is also necessary to identify the indicators or "clues" that lead to the CI items. For example, protecting the information on movement of key personnel can quickly be countered with arrangements for staff cars to meet arriving flights, preparation of DV quarters, etc. While this might not state which DV is traveling, these clues allow an adversary to focus attention on other collection means to obtain the CI items.